Christian Gomille

Der Feind in meinem Haus[1] (Vertragliche) Ansprüche auf Sicherheitsupdates

I. Einleitung

1. Einige Beispiele für Sicherheitsgefahren bei der Nutzung von Computersystemen

Nutzern eines Computersystems, das in ein Netzwerk eingebunden ist, dürfte bewusst sein, dass sie sich in der ständigen Gefahr befinden, dass ein Dritter, ihnen nicht freundlich Gesonnene über eine Schwachstelle in das Computersystem eindringt und dort Schaden anrichtet, indem er Daten ausspäht, Schadprogramme hinterlässt und/oder nutzerseitig nicht autorisierte Steuerungsbefehle erteilt und durch das System ausführen lässt. Und obwohl diese sog. „Cybergefahren" an sich notorisch sind, lässt es sich nicht vermeiden, dass sie sich dann und wann verwirklichen, wie sich anhand einiger ausgewählter Beispiele veranschaulichen lässt:

a) Der Angriff auf den Rhein-Pfalz-Kreis[2]

Als erstes Beispiel sei der Angriff auf den Rhein-Pfalz-Kreis aus dem Jahr 2022 erwähnt, der jedenfalls in den regionalen Medien einige Wellen geschlagen hat. Hier ist eine Hackergruppe namens „Vice Society" mutmaßlich über ein infiziertes Gerät – so ganz genau weiß man es bis heute nicht – in das Netzwerk der Kreisverwaltung eingedrungen, hat dort persönliche Daten von ca. 4.000 Personen ausgespäht und offenbar netzwerkweit auch allerhand Schadsoftware hinterlassen. Die IT-Abteilung der Kreisverwaltungsbehörde konnte immerhin noch einigermaßen rechtzeitig reagieren und – wie es der Landrat *Clemens Körner* ausdrückte – „abschalten, bevor wir abgeschaltet wurden."

---

[1] Der Text basiert auf einem Vortrag, den der Verfasser am 7. Februar 2023 im Rahmen der „Trierer Gespräche zu Recht und Digitalisierung" am IRDT der Universität Trier gehalten hat, die im Wintersemester 2022/2023 zu dem Generalthema „Sicherheitslücken" stattfanden. Die Vortragsform wurde weitgehend beibehalten. Sämtliche Internetquellen wurden zuletzt am 30. Oktober 2023 abgerufen.

[2] https://www.swr.de/swraktuell/rheinland-pfalz/ludwigshafen/hackerangriff-auf-rhein-pfalz-kreis-100.html.

Der Schaden ist aber auch so schon beträchtlich. Denn zum einen war die Kreisverwaltung in ihrer Tätigkeit über Wochen auf Stift und Papier zurückgesetzt. Und zum anderen müssen sämtliche 600 Rechner der Behörde verschrottet und ersetzt werden. Buchhalterisch schätzt man den entstandenen materiellen Schaden auf ca. 1,2 Millionen Euro.

b) Die Ransomware „WannaCry“[3]

Bei der Verwaltung des Rhein-Pfalz-Kreises geht man aktuell noch davon aus, dass man einem Erpressungsversuch durch die „Vice Society“ gerade eben noch entgangen sei. Andere von Attacken aus dem Internet Betroffene hatten in der Vergangenheit allerdings deutlich weniger Glück, insbesondere zu der Zeit, als die Ransomware „WannaCry“ global um sich griff. Dabei handelt es sich um ein Schadprogramm, das im Frühjahr 2017 massenhaft auftrat. Das Programm konnte über Schwachstellen von Windows-Betriebssystemen in fremde Computersysteme eindringen und befiel vornehmlich Rechner, auf denen Windows 7 oder Windows XP installiert war. Einmal in das System eingedrungen, verschlüsselte „WannaCry“ die Daten, zu denen es Zugang bekam, und die hinter der Attacke stehenden Angreifer verlangten von den Betroffenen ein Lösegeld, damit diese ihre Daten wieder freigeschaltet bekämen.

Das besonders Verheerende an „WannaCry“ war, dass es über die Verschlüsselung hinaus auch noch eine Wurmfunktion enthielt, über die es sich rasant und global ausbreiten konnte. Die wirtschaftlichen Schäden, die „WannaCry“ weltweit anrichtete, werden auf ca. 4 Milliarden US$ geschätzt.

c) Firmware mit sicherheitsrelevanten Schwachstellen

Dritte, die in das Computersystem des Nutzers eindringen und dort Schaden anrichten wollen, nutzen aber nicht nur die Schwachstellen von reinen Softwareprodukten aus, sondern auch Schwachstellen von Software, die in ein Gerät „eingebettet“ und funktional fest mit diesem verbunden ist. Wenn man sich die entsprechenden Meldeportale anschaut, dann sieht man, dass solche sog. Firmware von Routern offenbar ein besonders beliebtes Ziel von Angreifern ist.[4] Der Fantasie sind hier

[3] https://de.wikipedia.org/wiki/WannaCry.

[4] https://www.chip.de/news/Router-Updates-noetig-In-vielen-Modellen-Sicherheitsluecken-gefunden_184596147.html.

allerdings kaum irgendwelche Grenzen gesetzt. Besonders anschaulich ist in diesem Zusammenhang das Beispiel aus der Literatur von der Alarmanlage, deren Firmware fehlerhaft ist und die deshalb von Einbrechern per Fernzugriff ausgeschaltet werden kann.[5] Um im Bild des Vortragstitels zu bleiben: Hier stehen die Feinde dann nicht mehr nur virtuell, sondern ganz buchstäblich im Haus des Nutzers.

d) Hardwarebedingte Sicherheitslücken

Sicherheitslücken in Computersystemen haben ihre Ursache zwar sehr häufig, aber keineswegs zwingend immer nur in einer eingesetzten Software. Vielmehr kann durchaus auch einmal die Hardware das Problem sein. Berühmt-berüchtigte Beispiele hierfür sind die Sicherheitslücken, die unter den Bezeichnungen „Meltdown“[6] und „Spectre“[7] bekannt geworden sind. Als Einfallstür für die Angreifer dienten hier die Spezifika von zahlreichen Mikroprozessoren, etwa des Herstellers Intel, über die vor allem in dem betroffenen System gespeicherte Daten ausgespäht werden konnten.

Solche Hardwaresicherheitslücken können manchmal tatsächlich nur durch den physischen Austausch der betroffenen Komponente beseitigt werden. Sehr häufig kann der Hardwarefehler aber bereits durch eine Softwareaktualisierung kompensiert werden, die entweder die Firmware des Prozessors betrifft oder aber das Betriebssystem des Computers, in den der kritische Prozessor verbaut wurde.

2. Wie können sich Nutzer gegen solche Angriffe wappnen?

Vor diesem Hintergrund stellt sich die Frage, wie die Nutzer von an Netzwerke angeschlossenen Computersystemen sich gegen solche Gefahren von außen sichern können und welche Rolle vor allem vertragliche Ansprüche auf Sicherheitsaktualisierungen dabei spielen.

Insoweit kann man zunächst einmal sicher davon ausgehen, dass jeder Nutzer sich darüber im Klaren ist, dass vernetzte Computersysteme verletzlich und ständigen Bedrohungen von außen ausgesetzt sind. Dementsprechend werden die Nutzer in der Regel auch die ihnen möglichen Vorkehrungen treffen, damit diese Gefahren sich tunlichst nicht verwirklichen und der Feind draußen vor der

5 Vgl. *Heydn*, CR 2021, 709 Rn. 17
6 https://de.wikipedia.org/wiki/Meltdown_(Sicherheitslücke).
7 https://de.wikipedia.org/wiki/Spectre_(Sicherheitsllücke).

virtuellen Türe bleibt. Dazu gehören natürlich der Einsatz von Firewalls und von regelmäßig aktualisierten Virenscannern, aber auch, dass man Dateien aus unbekannten oder unseriösen Quellen besser nicht öffnet. In Zusammenhang mit den eigenen Verkehrssicherungspflichten im Verhältnis zu anderen an ein Netzwerk angeschlossenen Nutzern geht man sogar davon aus, dass der Einsatz eines regelmäßig aktualisierten Virenscanners sowie einer Firewall zur notwendigen Basisausstattung eines jeden Nutzers zählt.[8]

Allerdings wird der Nutzer selbst bei Beachten der idealen Sorgfalt alleine nicht in der Lage sein, die durch Schwachstellen/Sicherheitslücken der Software oder Hardware drohenden Gefahren effektiv abzuwehren. Hierzu benötigt er vielmehr die Unterstützung seiner Vertragspartner und ggf. auch der Hersteller, die ihm – wann immer erforderlich – Sicherheitsaktualisierungen zur Verfügung stellen, mit denen sich zwischenzeitlich bekannt gewordene Sicherheitslücken schließen lassen.[9] Und tatsächlich sieht das bürgerliche Recht mittlerweile eine ganze Reihe von Mitteln und Wegen vor, wie der Nutzer an solche Sicherheitsaktualisierungen kommen kann. Sie sollen im Rahmen dieses Beitrags kursorisch vorgestellt werden. Dabei gilt es zunächst, den rechtlichen Rahmen zu umreißen, also die Anspruchsgrundlagen aufzuzeigen, aufgrund derer der Nutzer von einem anderen die Bereitstellung einer Sicherheitsaktualisierung verlangen kann. In diesem Zusammenhang wird festzustellen sein, dass nach dem (dispositiven) Gesetzesrecht zwischen Ansprüchen auf Beseitigung anfänglicher und nachträglicher Sicherheitslücken zu unterscheiden ist. Diese beiden Anspruchsgruppen sollen sodann noch kurz vorgestellt werden.

II. Der rechtliche Rahmen

Zunächst also zu dem rechtlichen Rahmen. Insoweit haben sich in Umsetzung der Digitale-Inhalte-Richtlinie[10] und der Warenkaufrichtlinie[11] in das deutsche

8 LG Köln, MMR 2008, 259, 261; LG Nürnberg-Fürth, BeckRS 2008, 26304; vgl. auch KG MMR 2011, 338, 339.

9 *Raue*, NJW 2017, 1841, 1843.

10 Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, Abl. EU L 136/1.

11 Richtlinie (EU) 2019/771 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs, zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie 2009/22/EG sowie zur Aufhebung der Richtlinie 1999/44/EG, Abl. EU L 136/28.

Recht zum 1. Januar 2022[12] einige ganz wesentliche und in der Sache durchaus sinnvolle Neuerungen ergeben, die in ihrer konkreten Ausgestaltung allerdings stark ausdifferenziert und damit nicht unbedingt übersichtlich geraten sind.

1. Verbraucherverträge über die Bereitstellung eines digitalen Produkts

a) Allgemeines

Zuallererst sind dabei natürlich die Verträge zu nennen, bei denen gemäß § 327 Abs. 1 BGB ein Unternehmer einem Verbraucher gegen Zahlung eines Preises ein digitales Produkt bereitstellt. Unter den Oberbegriff des digitalen Produkts fallen dabei die in § 327 Abs. 2 Satz 1 BGB legaldefinierten digitalen Inhalte ebenso wie die digitalen Dienstleistungen, deren Legaldefinition man in § 327 Abs. 2 Satz 2 BGB findet.

Software als solche fällt dabei gewiss unter den Begriff des digitalen Produkts.[13] Ob sie nun aber ein digitaler Inhalt oder eine digitale Dienstleistung ist, lässt sich nicht einheitlich beurteilen. Entscheidend ist vielmehr die Art und Weise der Bereitstellung im konkreten vertraglichen Kontext. Erhält der Verbraucher die Software etwa dauerhaft zur eigenen Nutzung auf einem eigenen Datenträger überlassen, wird man sie unter die digitalen Inhalte nach § 327 Abs. 2 Satz 1 BGB subsumieren.[14] Eröffnet der Unternehmer dem Verbraucher demgegenüber lediglich die Möglichkeit, die Software über eine Cloud-Lösung zu nutzen – der Richtliniengeber spricht insoweit von „Software as a Service" –,wird man insoweit eine digitale Dienstleistung anzunehmen haben.[15]

Für die Frage nach den Unternehmerpflichten ist diese Zuordnung letztlich aber nur in Randbereichen der §§ 327 ff. BGB entscheidend. Diese definieren für den Unternehmer nämlich ein Leistungsprogramm, das – jedenfalls weitgehend – von der Art des digitalen Produkts ebenso unabhängig ist wie von der typologischen Zuordnung des Vertrags etwa als Kauf-, Werk-, Miet- oder als Herstellerleasingvertrag.

---

[12] Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen vom 25. Juni 2021, BGBl. I, S. 2123.

[13] MüKoBGB/*Metzger* (9. Aufl. 2022), § 327 Rn. 7; s. auch Erwägungsgrund 19 zur RL (EU) 2019/770.

[14] *Riehm*, RDi 2022, 209 Rn. 9.

[15] *Riehm*, RDi 2022, 209 Rn. 9; s. auch Erwägungsgrund 19 zur RL (EU) 2019/770.

b) Zwei Anspruchsgrundlagen für die Bereitstellung von Sicherheits-Updates innerhalb der §§ 327 ff. BGB

Und wenn man sich dieses durch §§ 327 ff. BGB definierte Leistungsprogramm des Unternehmers einmal genauer anschaut, dann stößt man auf zwei Anspruchsgrundlagen, aufgrund derer der Verbraucher von seinem Vertragspartner die Bereitstellung einer Sicherheitsaktualisierung seiner Software verlangen kann.

Ausgangspunkt ist § 327d i.V.m. § 327e Abs. 1 Satz 1 BGB, wonach der Unternehmer dem Verbraucher das digitale Produkt so bereitzustellen hat, dass es den subjektiven Anforderungen, den objektiven Anforderungen und den Anforderungen an die Integration entspricht. Zu den objektiven Anforderungen gehört dabei gemäß § 327e Abs. 3 Nr. 2 BGB ausdrücklich der Sicherheitsstandard, der bei digitalen Produkten derselben Art üblich ist und den der Verbraucher unter Berücksichtigung der Art des digitalen Produkts erwarten kann. Der Verbraucher hat demnach also zunächst einen primären Leistungsanspruch, dass die ihm bereitzustellende Software bis zu einem gewissen, später noch näher zu konkretisierenden Grad frei von sicherheitsrelevanten Schwachstellen ist. Und daraus folgt dann, dass ein digitales Produkt, das im maßgeblichen Zeitpunkt der Bereitstellung (§ 327b Abs. 3 BGB) diesen Sicherheitsstandard nicht erreicht, schon anfänglich mangelhaft ist und der Verbraucher gegen den Unternehmer deshalb einen Anspruch auf Nacherfüllung aus § 327l i.V.m. § 327i Nr. 1 BGB hat. Wie der Unternehmer diesem gegen ihn gerichteten Nacherfüllungsanspruch gerecht wird, ist dabei anders als im Kaufrecht ihm selbst überlassen.[16] Es liegt aber mehr als nahe, dass er diesen Anspruch des Verbrauchers entweder durch die Bereitstellung einer Sicherheitsaktualisierung der Software oder aber durch die Bereitstellung einer neuen Version, die den geschuldeten Sicherheitsstandard erreicht, erfüllen wird.

Aber: Im Hinblick auf die Sicherheit der bereitgestellten Software hat der Unternehmer damit seine Pflichten gegenüber dem Verbraucher noch lange nicht endgültig erfüllt. Aus § 327f Abs. 1 Sätze 1 und 2 BGB ergibt sich nämlich, dass der Unternehmer während des nach § 327f Abs. 1 Satz 3 BGB maßgeblichen Zeitraums zugunsten des Verbrauchers die Bereitstellung von Aktualisierungen sicherzustellen hat, die im Vertrag vereinbart oder – und das ist das eigentlich Spannende an dieser Vorschrift – für den Erhalt des üblichen und erwartbaren Sicherheitsstandards

[16] *Heydn*, CR 2021, 709 Rn. 14.

des digitalen Produkts erforderlich sind. Tut der Unternehmer das nicht, wird das digitale Produkt gemäß § 327e Abs. 2 Nr. 3 BGB bzw. gemäß § 327e Abs. 3 Nr. 5 BGB nachträglich mangelhaft und der Verbraucher erhält gegen den Unternehmer wiederum einen Anspruch auf Nacherfüllung aus § 327l i.V.m. § 327i Nr. 1 BGB.[17]

c) Paketverträge etc.

Diese beiden Nacherfüllungsansprüche betreffen unmittelbar zunächst nur den Fall, dass der Vertrag nach § 327 Abs. 1 BGB die Bereitstellung eines reinen Softwareprodukts zum Gegenstand hat. Aus § 327a Abs. 1 und 2 BGB ergibt sich aber, dass der Verbraucher in Bezug auf die Software diese beiden Formen der Nacherfüllung auch dort verlangen kann, wo die Software entweder – wie es im Gesetz heißt – im „Paket" mit Sachen oder Dienstleistungen vertrieben wird oder in einer Sache als Vertragsgegenstand enthalten oder mit dieser verbunden ist.[18] Beispiele dafür sind etwa der Erwerb eines Netflix-Abos zusammen mit dem Erwerb eines neuen Fernsehgeräts oder einer App zusammen mit dem Abschluss eines Nutzungsvertrags mit einem Fitnessstudio.

2. Verbrauchsgüterkaufverträge über Waren mit digitalen Elementen

Grundsätzlich sind demnach die §§ 327 ff. BGB also unabhängig davon anwendbar, ob dem Verbraucher die Software allein oder zusammen mit anderen Leistungen des Unternehmers bereitgestellt wird. Wie so häufig gilt aber auch hier: Keine Regel ohne Ausnahme. Insbesondere die Firmware-Fälle unterwirft der Gesetzgeber über § 327 Abs. 3 BGB den kaufrechtlichen Bestimmungen, präziser gesagt: den Bestimmungen über den Verbrauchsgüterkaufvertrag.[19] Diese Ausnahme hat ihren Grund in der notwendigen Abstimmung der Anwendungsbereiche von Digitale-Inhalte-Richtlinie und Warenkaufrichtlinie, bedeutet inhaltlich aber natürlich nicht, dass der Verbraucher hier keinen Anspruch auf die Beseitigung von Mängeln in Form von sicherheitsrelevanten Schwachstellen der Firmware hätte. Für den Fall eines anfänglichen Mangels ergibt sich der Nacherfüllungsanspruch dann aber aus § 439 Abs. 1, § 437 Nr. 1 i.V.m. § 475b Abs. 4 Nr. 1 und § 434 Abs. 3 Nr. 2 BGB. Nach Maßgabe von § 475b Abs. 4 Nr. 2 BGB kann aber auch eine Ware

[17] MüKoBGB/*Metzger* (9. Aufl. 2022), § 327f Rn. 2.
[18] *Wendehorst*, NJW-Sonderausgabe: Neues Schuldrecht/2021, 17 Rn. 7.
[19] *Wiesemann*, MMR 2022, 343.

mit digitalen Elementen nachträglich aktualisierungsbedürftig werden, wenn sie nach dem Gefahrübergang ihre vertragsgemäße Beschaffenheit, insbesondere im Hinblick auf die Sicherheit, verliert. Hier ergibt sich der Nacherfüllungsanspruch des Verbrauchers dann aus §§ 439 Abs. 1 i.V.m. § 437 Nr. 1 und § 475b Abs. 4 Nr. 2 BGB.[20]

Danach hat der Verbraucher gegen den Unternehmer grundsätzlich auch in den Ausgangsbeispielen des Routers und der Alarmanlage grundsätzlich einen Anspruch auf Sicherheitsupdates, nur eben nicht auf Grundlage von §§ 327 ff. BGB. Hinzuweisen ist freilich darauf, dass die §§ 327 ff. BGB auf eine Ware mit digitalen Elementen dann doch wieder anwendbar werden, wenn der Verbraucher diese aufgrund eines anderen Vertrags als einem Kaufvertrag überlassen bekommt.[21] Der Hintergrund dafür ist, dass im Hinblick auf diese anderen Vertragstypen von vornherein keine Abstimmung zwischen der Digitale-Inhalte-Richtlinie einerseits und der Warenkaufrichtlinie andererseits erforderlich ist.

3. Andere Verträge als Verbraucherverträge

Leider – manche sagen allerdings auch „zum Glück!“ – gilt das besondere digitale Vertrags- und Leistungsstörungsrecht aber nur bei Verbrauchergeschäften. Das bedeutet, dass Verträge über Software und Waren mit digitalen Inhalten insbesondere im unternehmerischen Verkehr mit den allgemeinen Bordmitteln des bürgerlichen Rechts erfasst werden müssen.[22] Deshalb wird hier die typologische Zuordnung des Vertrags dann doch wieder relevant[23] und es ergibt sich wegen der Ansprüche auf Beseitigung sicherheitsrelevanter Schwachstellen eines digitalen Produkts folgendes Bild:

- Überlässt die eine Vertragspartei der anderen eine Software oder eine Ware mit digitalen Elementen aufgrund eines Miet- oder eines Herstellerleasingvertrags, so ergibt sich der Anspruch des Mieters bzw. Leasingnehmers auf Beseitigung eines anfänglichen Sicherheitsmangels aus § 535 Abs. 1 Satz 1 BGB. Die Beseitigung später entstehender Sicherheitsmängel kann der Mieter bzw. Leasingnehmer von seinem Vertragspartner ebenfalls verlangen, und zwar

[20] *Felsch/Kremer/Wagener*, MMR 2022, 18, 20.
[21] *Felsch/Kremer/Wagener*, MMR 2022, 18, 19.
[22] *Heydn*, CR 2021, 709 Rn. 50.
[23] *Heydn*, CR 2021, 709 Rn. 51.

aufgrund von § 535 Abs. 1 Satz 2 BGB.[24]

- Handelt es sich bei dem Vertrag hingegen um einen Kauf- oder um einen Werkvertrag, sieht das dispositive Gesetzesrecht ausdrücklich zunächst nur Nacherfüllungsansprüche aus § 439 Abs. 1 i.V.m. § 437 Nr. 1 und § 453 Abs. 1 BGB bzw. aus § 635 Abs. 1 i.V.m. § 634 Nr. 1 BGB wegen bereits bei Gefahrübergang bestehender Mängel vor. Die von Gesetzes wegen hier zunächst nicht vorgesehenen Aktualisierungspflichten haben manche Instanzgerichte dann versucht, dem § 241 Abs. 2 BGB zu entnehmen.[25] Im Übrigen sind sie Gegenstand individueller Vereinbarungen zwischen den jeweiligen Vertragsparteien („Softwarepflegevertrag“).[26]

III. Nacherfüllungsansprüche auf Beseitigung eines anfänglichen (Sicherheits-)Mangels

1. Ausgangspunkt

Wenn ein vertraglicher Anspruch auf Bereitstellung einer Sicherheitsaktualisierung zunächst ein Anspruch auf Beseitigung eines anfänglichen Mangels einer Software oder einer Ware mit digitalen Elementen sein kann, dann ist im Ausgangspunkt zunächst dieser Anspruch näher zu betrachten. Hier ist – unabhängig von der im konkreten Fall jeweils heranzuziehenden Anspruchsgrundlage – stets erforderlich, dass die Software oder die Ware mit digitalen Elementen im maßgeblichen Zeitpunkt der Bereitstellung, der Überlassung oder des Gefahrübergangs einen Mangel aufweist. Ein solcher liegt übergreifend für alle zuvor genannten Vertragstypen vor, wenn der Vertragsgegenstand nicht die Beschaffenheit hat, die er nach dem Inhalt des vertraglichen Versprechens eigentlich haben sollte. Bricht man das weiter auf die Frage nach den zur Mängelbeseitigung erforderlichen Sicherheitsaktualisierungen herunter, so ist im Ausgangspunkt also zu ermitteln, welches Maß an Sicherheit gegen virtuelle Eindringlinge von außen Software und Waren mit digitalen Elementen aufweisen müssen, um vertragsgemäß zu sein.

[24] Vgl. Schneider/*Schneider*, Handbuch des EDV-Rechts (5. Aufl. 2017), Rn. R 540.
[25] OLG Koblenz, NJW-RR 1993, 636; LG Köln, NJW-RR 1999, 1285.
[26] Schneider/*Schneider/Kahlert*, Handbuch des EDV-Rechts (5. Aufl. 2017), Rn. S 1.

2. Die Ermittlung der Soll-Beschaffenheit anhand des bei Vertragsgegenständen derselben Art Üblichen und berechtigterweise Erwartbaren

Nun hat der Gesetzgeber die Sicherheit des digitalen Produkts durch § 327e Abs. 3 Nr. 2 BGB zwar in den Katalog der mängelrelevanten Beschaffenheitsmerkmale aufgenommen, sich im Übrigen aber jeder weiteren Konkretisierung enthalten.

Natürlich sind insoweit die konkreten vertraglichen Abreden als subjektive Anforderungen an den Vertragsgegenstand zu beachten. Hier besteht an sich ein recht großer privatautonomer Gestaltungsspielraum. Zu beachten ist freilich, dass die objektive Anforderung gem. § 327e Abs. 3 Satz 1 Nr. 2 BGB eine Mindestanforderung darstellt, die – vorbehaltlich des für Sicherheitsfragen praktisch nicht relevanten § 327h BGB – durch abweichende, subjektiv vereinbarte Anforderungen nicht unterschritten werden darf.[27] Diese objektive Anforderung des bei Vertragsgegenständen derselben Art Üblichen und Erwartbaren definiert damit einen gewissen Mindeststandard, der nicht nur im Kauf-, Werk- und Digitalvertragsrecht gesetzlichen Niederschlag gefunden hat, sondern auch im Mietrecht zur Bestimmung der Soll-Beschaffenheit dient.

a) Gibt es bei Softwareprodukten überhaupt eine übliche und erwartbare Soll-Beschaffenheit?

Freilich wurde in Bezug auf Softwareprodukte früher tatsächlich vereinzelt vertreten, dass hier eine Ermittlung der Soll-Beschaffenheit anhand der objektiven Kriterien von Üblichkeit und Erwartbarkeit wegen der Eigenart des Vertragsgegenstands von vornherein ausscheiden müsse.[28] Diese aus den 1990er Jahren stammende Auffassung war natürlich von Anfang an zweifelhaft, seit der Einführung des § 453 Abs. 1 BGB zum 1.1.2002, durch den die grundsätzliche Anwendbarkeit von Kaufrecht auf zur dauerhaften Überlassung eines Vervielfältigungsstücks einer Software verpflichtende Verträge klargestellt werden sollte,[29] allenfalls noch mit Mühe aufrechtzuerhalten; spätestens mit der Beschreibung des Produktmangels in § 327e BGB hat sie aber jede Grundlage verloren.

---

27 MüKoBGB/*Metzger* (9. Aufl. 2022), § 327e Rn. 25.

28 Vgl. *Marly*, Praxishandbuch Softwarerecht (7. Aufl. 2018), Rn. 1450, der referiert, dass das OLG Stuttgart diese Auffassung in seiner Rechtsprechung vertreten habe, dafür aber leider keine Fundstelle benennt.

29 S. nur Jauernig/*Berger*, BGB (18. Aufl. 2021), § 453 Rn. 11.

Dabei ist es aber in der Tat nicht gerade einfach, einen solchen objektiven Maßstab zu definieren, was häufig mit der rasanten technischen Entwicklung begründet wird.[30] Ausgangspunkt für eine objektive Soll-Beschaffenheit sei jenseits gewisser Minimalanforderungen deshalb die Bildung von Leistungsklassen, aufgrund von deren vergleichender Betrachtung ein IT-Sachverständiger dann übliche und erwartbare Beschaffenheitsmerkmale definieren könne.[31]

b) Berechtigte Erwartung von absoluter Sicherheit?

Vielleicht könnte man es sich aber mit Blick auf die übliche und erwartbare Abwesenheit von sicherheitsrelevanten Schwachstellen einer Software demgegenüber auch ganz einfach machen und schlicht die absolute Sicherheit der Software oder des sonstigen digitalen Produkts für legitimerweise erwartbar erklären. In diesem Fall dürfte der Vertragsgegenstand dann erstens natürlich keine Schwachstellen aufweisen, die bereits zur Zeit seiner Bereitstellung an den Nutzer bekannt sind. Zweitens wäre er aber auch wegen erst später als solcher erkennbarer Schwachstellen als von Anfang an mangelhaft anzusehen. Konstruierbar wäre solch ein anfänglicher Mangelbegriff durchaus, und zwar indem man annimmt, dass jeder auch erst später erkennbare Mangel im maßgeblichen Zeitpunkt der Bereitstellung, der Überlassung oder des Gefahrübergangs wenigstens im Kern angelegt war.[32]

Tatsächlich ist dieser Weg zur Bestimmung der Sollbeschaffenheit – auch wenn er noch so verführerisch einfach klingen mag – aber gleich aus mehreren Gründen nicht gangbar. Zunächst bestünde die Konsequenz nämlich darin, dass jede sicherheitsrelevante Schwachstelle, die erst nach Bereitstellung, Überlassung oder Gefahrübergang aber während der offenen Verjährungsfrist erkennbar wird, einen anfänglichen Mangel darstellte und bei Verbraucherverträgen bereits aufgrund von § 327l i.V.m. § 327i Nr. 1 und § 327e Abs. 3 Nr. 2 BGB zu ersetzen wäre. Für § 327f BGB bliebe dann nur noch Raum für sicherheitsrelevante Schwachstellen, die erst nach dem Ablauf der Verjährungsfrist bekannt werden. Bei Softwaremietverträgen zwischen Unternehmern wäre § 535 Abs. 1 Satz 2 BGB sogar völlig gegenstandslos. Das beides kann aber schwerlich den Intentionen des Gesetzgebers entsprechen.

Es kommt hinzu, dass Software – auch hinsichtlich ihrer Absicherung gegen Angriffe

[30] *Marly*, Praxishandbuch Softwarerecht (7. Aufl. 2018), Rn. 1450.
[31] *Marly*, Praxishandbuch Softwarerecht (7. Aufl. 2018), Rn. 1450.
[32] Vgl. OLG Schleswig, NJW-RR 2009, 1065, 1066.

von außen – anerkanntermaßen niemals vollkommen fehler- und schwachstellenfrei programmiert werden kann.[33] Ein Sicherheitsstandard aber, den ein digitales Produkt bereits seiner Art nach von vornherein nicht erreichen kann, kann auch nicht die übliche Beschaffenheit eines solchen Produkts definieren.[34]

c) Programmierung gemäß dem Stand der Technik

Wenn die Soll-Beschaffenheit einer Software im Hinblick auf ihre Sicherheit danach nicht mit vollkommener Freiheit von sicherheitsrelevanten Schwachstellen übersetzt werden kann, dann stellt sich die Frage, wie man stattdessen die objektiv übliche und vom Nutzer vernünftigerweise erwartbare Sicherheitsbeschaffenheit einer Software juristisch so beschreiben kann, dass sie in einem etwaigen Prozess unter Hinzuziehung eines Sachverständigen handhabbar wird.

Der BGH hat in Bezug auf die werkvertragliche Mängelhaftung in der Vergangenheit schon mehrfach davon gesprochen, dass eine Software jedenfalls dem Stand der Technik bei einem mittleren Ausführungsstandard genügen müsse.[35] In der obergerichtlichen Rechtsprechung finden sich entsprechende Aussagen auch vor dem Hintergrund der kaufrechtlichen Mängelhaftung.[36] Diese Bestimmung der objektiven Soll-Beschaffenheit nimmt mit dem Abstellen auf den Stand der Technik letztlich Anleihen beim produkthaftungsrechtlichen Fehlerbegriff des § 3 ProdHaftG.[37] Der damit einhergehende wenigstens näherungsweise Gleichlauf zwischen dem produkthaftungsrechtlichen Fehler und dem vertragsrechtlichen Mangel erscheint durchaus plausibel. Denn erstens schützt § 3 ProdHaftG die legitimen Sicherheitserwartungen des Verkehrs an ein Produkt zur Zeit der Inverkehrgabe durch den Hersteller und es leuchtet nicht ein, weshalb die legitimen Sicherheitserwartungen eines Verkehrsteilnehmers andere sein sollten, wenn er dasselbe, neuwertige Produkt später von einem Vertragspartner überlassen bekommt.

---

33 S. etwa Leupold/Wiebe/Glossner/*Wiesner*, IT-Recht (4. Aufl. 2021), Teil 10.6 Rn. 41; *Günther*, Produkthaftung für Informationsgüter (2001), S. 208; *Raue*, NJW 2017, 1841; *Rockstroh/Peschel*, NJW 2020, 3345 Rn. 1

34 Vgl. Jauernig/*Mansel*, BGB (18. Aufl. 2021), § 633 Rn. 6; Rn. Taeger/Pohle/*Ammann*, Computerrechts-Handbuch (Stand: Mai 2022), Teil 32.2 Rn. 61; *Riehm/Abold*, CR 2021, 530 Rn. 49.

35 BGH, NJW-RR 1992, 556, 557; 2004, 782, 783; wohl zust. *Lejeune*, ITRB 2023, 18, 25.

36 OLG Brandenburg, CR 1999, 748, 749; ebenso Schuster/Grützmacher/*Diedrich*, IT-Recht (1. Aufl. 2020), § 434 Rn. 25.

37 Vgl. BeckOGK BGB/*Goehl* (Stand: 1.10.2022), § 3 ProdHaftG Rn. 64.

Und zweitens hat die Rechtsprechung auch in Bezug auf andere Vertragsgegenstände den üblichen und erwartbaren Sicherheitsstandard dem Stand der Technik entlehnt, und zwar namentlich in Bezug auf den Kauf von Kraftfahrzeugen.[38]

Gegen dieses Vorgehen bei der Bestimmung der Soll-Beschaffenheit einer Software wurde nun zwar gelegentlich eingewandt, dass es gewissermaßen den Goldsicherheitsstandard des Branchenprimus‘ für eine gesamte Branche verbindlich setze, was aber unverhältnismäßig sei.[39] Doch dürfte diesem Einwand ein zu strenges Verständnis vom Stand der Technik und den daraus abzuleitenden Sicherheitserwartungen des Verkehrs oder des einzelnen Nutzers zugrunde liegen. Denn natürlich bietet ein Mercedes der G-Klasse beim Aufprall auf ein Hindernis dem Fahrer eine ganz andere Sicherheit als ein Smart. Ebenso natürlich können beide Fahrzeugtypen aber dem Stand der Technik entsprechen und damit beide unter Sicherheitsaspekten fehler- und mangelfrei sein.[40] Das folgt daraus, dass der Stand der Technik stets für jede Produktklasse selbständig zu ermitteln ist[41] und die beiden im Beispiel genannten Fahrzeuge nun einmal unterschiedlichen Klassen zuzuordnen sind.

Letztlich kommt man hier deshalb nicht umhin, das im Hinblick auf die Sicherheit der Software Übliche und Erwartbare zu ermitteln, indem man zuerst eine Vergleichsklasse bildet, sodann schaut, welche möglichen und zumutbaren Sorgfaltsvorkehrungen ein vernünftiger Hersteller bei der Programmierung eines solchen Softwareprodukts walten ließe und dies schließlich abstimmt auf die – wie es in der Literatur heißt – Gefahrsteuerungspotentiale des Nutzers, für die wiederum der angesprochene Verkehrskreis und nicht zuletzt auch der Preis des Produkts von Bedeutung sind.[42] Konkret bedeutet das, dass die Software jedenfalls mangelhaft ist, wenn sie bei Bereitstellung, Überlassung oder Gefahrübergang eine sicherheitsrelevante Schwachstelle aufweist, die zu dieser Zeit bereits bekannt ist. Sie ist darüber hinaus aber auch in Bezug auf bei Bereitstellung, Überlassung

[38] OLG Hamm, NJW-RR 2009, 485, 486; zust. jurisPK-BGB/*Pammler* (10. Aufl. 2023), § 434 Rn. 115; MüKoBGB/*Westermann* (8. Aufl. 2019), § 434 Rn. 62; Staudinger/*Matusche-Beckmann*, BGB (2013), § 434 Rn. 90.

[39] *Rockstroh/Peschel*, NJW 2020, 3345 Rn. 21.

[40] Vgl. MüKoBGB/*Wagner* (8. Aufl. 2020), § 823 Rn. 956.

[41] OLG Karlsruhe, NJW-RR 2008, 137, 138; OLG Hamm, NJW-RR 2009, 485, 486; OLG München, NJW-RR 2023, 274 Rn. 22.

[42] MüKoBGB/*Wagner* (8. Aufl. 2020), § 823 Rn. 954.

und Gefahrübergang zwar objektiv vorhandene, aber noch nicht entdeckte sicherheitsrelevante Schwachstellen mangelhaft, wenn diese Schwachstellen nach dem Stand der Technik für die konkrete Produktklasse hätten erkannt und damit vermieden werden können.

d) Die Feststellung des anfänglichen Mangels und ihr Verhältnis zur Aktualisierungspflicht wegen nachträglich aufgetretener Sicherheitslücken

Die Feststellung von Letzterem mag dabei im Prozess gewiss mit einigen Schwierigkeiten und Unsicherheiten verbunden sein. Immerhin wirkt dieses Problem sich aber jedenfalls, was den Nacherfüllungsanspruch anbelangt, praktisch nicht aus, wenn die Software oder die Ware mit digitalen Inhalten aufgrund eines Verbrauchervertrags gemäß § 327 Abs. 1, § 327a Abs. 1 oder Abs. 2 bzw. aufgrund eines Verbrauchsgüterkaufvertrags über eine Ware mit digitalen Elementen überlassen wurde.[43] Sobald nämlich in diesen Fällen nach der Bereitstellung oder dem Gefahrübergang eine sicherheitsrelevante Schwachstelle der Software zutage tritt, wird die Pflicht aus § 327f BGB zur Bereitstellung einer Sicherheitsaktualisierung aktuell; verletzt der Unternehmer seine Pflicht, eine solche Bereitstellung sicherzustellen, so wird die Software nach dem soeben Gesagten automatisch nachträglich mangelhaft und der Nacherfüllungsanspruch des Verbrauchers resultiert jedenfalls aus § 327l, § 327i Nr. 1 i.V.m. § 327e Abs. 3 Nr. 2 und § 327f BGB bzw. aus § 439 Abs. 1, § 437 Nr. 1 i.V.m. § 475b Abs. 4 Nr. 2 BGB.

Im Ergebnis Gleiches gilt, wenn die Software außerhalb eines Verbrauchervertrags aufgrund eines Miet- oder Herstellerleasingvertrags zur Verfügung gestellt wird. Hier ist der nachträglich entstandene Mangel nämlich aufgrund von § 535 Abs. 1 Satz 2 BGB zu beseitigen.

In allen anderen Fällen – insbesondere bei Kauf- und Werkverträgen über Software oder Waren mit digitalen Elementen zwischen Unternehmern – muss man schon beim Nacherfüllungsanspruch zur Beseitigung eines anfänglichen Mangels die Frage beantworten, ob die später entdeckte sicherheitsrelevante Schwachstelle durch eine unterhalb des geschuldeten Sicherheitsstandards liegende Programmierung verursacht ist und deshalb einen schon bei Gefahrübergang bestehenden, also einen anfänglichen Mangel darstellt. Hier entgeht man diesem Problem nur, wenn

[43] Vgl. im Einzelnen MüKoBGB/*Metzger* (9. Aufl. 2022), § 327f Rn. 6.

die Parteien Ansprüche auf Sicherheitsaktualisierungen individuell vereinbart haben oder man aber mit einigen Instanzgerichten annimmt, dass sich auch im unternehmerischen Verkehr eine Pflicht zur Bereitstellung von Sicherheitsupdates jedenfalls aus § 241 Abs. 2 BGB ableiten lässt.

IV. Sicherheitsaktualisierungen gemäß § 327f BGB

Aufgrund von § 327f Abs. 1 BGB hat der Unternehmer die Bereitstellung von Sicherheitsaktualisierungen sicherzustellen, sofern, soweit und sobald sie für den Erhalt der Vertragsmäßigkeit eines digitalen Produkts, insbesondere einer Software, erforderlich sind. Wie bereits erwähnt, betrifft diese Unternehmerpflicht alle Verbraucherverträge gemäß § 327 Abs. 1 sowie § 327a Abs. 1 und 2 BGB. Für Verbrauchsgüterkaufverträge über Waren mit digitalen Inhalten gilt § 327f BGB zwar nicht direkt.[44] Allerdings liegt eine entsprechende Verpflichtung des Unternehmers dem § 475b Abs. 4 Nr. 2 BGB zugrunde.[45] In keinem Fall hat der Verbraucher allerdings einen primären Leistungsanspruch auf Bereitstellung einer Sicherheitsaktualisierung zu einem bestimmten Zeitpunkt.[46] Vielmehr gewährt das Gesetz dem Verbraucher lediglich einen Nacherfüllungsanspruch gegen den Unternehmer, wenn dieser die Bereitstellung der erforderlichen Aktualisierung nicht sicherstellt.

1. Die erforderliche Aktualisierung

Das führt unmittelbar zu der ersten entscheidenden Frage, nämlich wann die Bereitstellung einer Sicherheitsaktualisierung für die Software oder die Ware mit digitalen Elementen zugunsten des Verbrauchers erforderlich wird und deshalb von dem Unternehmer sicherzustellen ist.

a) Zwischenzeitlich bekannt gewordene Sicherheitslücken

Dem Gesetz ist hierzu in § 327f Abs. 1 Satz 1 sowie in § 475b Abs. 4 Nr. 2 BGB zunächst zu entnehmen, dass diese Pflicht dann entsteht, wenn die Aktualisierung erforderlich ist, um die Vertragsgemäßheit des Softwareprodukts oder der Ware mit digitalen Elementen aufrechtzuerhalten. Das bedeutet, dass dem Verbraucher

44 *Felsch/Kremer/Wagener*, MMR 2022, 18, 21.
45 *Riehm/Abold*, CR 2021, 530 Rn. 47.
46 *Riehm/Abold*, CR 2021, 530 Rn. 48.

jedenfalls immer dann eine Aktualisierung bereitzustellen ist, wenn die Software oder die Ware mit digitalen Elementen nach der ursprünglichen Bereitstellung an den Verbraucher bzw. nach dem Gefahrübergang nicht mehr der ursprünglich geschuldeten Soll-Beschaffenheit im Hinblick auf die Sicherheit gegen Eindringlinge von außen entspricht.[47] Spätestens also, sobald eine sicherheitsrelevante Schwachstelle öffentlich bekannt wird, wird zugleich eine Sicherheitsaktualisierung für den Verbraucher erforderlich.

b) Aktive Beobachtungspflichten

Praktisch problematisch ist daran freilich, dass Sicherheitslücken in Softwareprodukten und Waren mit digitalen Elementen häufig nicht sofort behoben werden können, sondern die Programmierung der Aktualisierung eine gewisse Zeit in Anspruch nimmt, und zwar schon aus dem Grund, dass durch ein allzu eilig aufgesetztes Update nicht neue Sicherheitslücken entstehen.

Für den Verbraucher entsteht damit das Problem, dass seine Software oder seine Ware mit digitalen Elementen während der gesamten Zeit zwischen dem öffentlichen Bekanntwerden der Sicherheitslücke und der Bereitstellung der Aktualisierung nicht der vertraglich geschuldeten Soll-Beschaffenheit entspricht, obwohl § 327f BGB doch gerade der Erhaltung[48] der Soll-Beschaffenheit des Vertragsgegenstands dient und eben nicht darauf beschränkt ist, die Wiederherstellung des vertragsmäßigen Zustands zu irgendeinem in ungewisser Zukunft liegenden Zeitpunkt in Aussicht zu stellen.

Dieser Erhaltungszweck des § 327f BGB legt deshalb die Annahme nahe, dass man für die Erforderlichkeit einer Sicherheitsaktualisierung nicht erst auf den Zeitpunkt des öffentlichen Bekanntwerdens einer Schwachstelle abstellen kann, sondern zeitlich früher ansetzen muss. Anknüpfen könnte man dabei an die produzentenhaftungsrechtlichen Produktbeobachtungspflichten, die der Hersteller ohnehin zu befolgen hat, um fortlaufend die Fehlerfreiheit seines Produkts i.S.d. § 3 ProdHaftG zu gewährleisten.[49] Erforderlich ist die Sicherheitsaktualisierung demnach schon in dem Moment, in dem der Hersteller bei Beachtung seiner

[47] BeckOK BGB/*Wendland* (Stand: 1.8.2022), § 327f Rn. 8; MüKoBGB/*Metzger* (9. Aufl. 2022), § 327f Rn. 4.
[48] MüKoBGB/*Metzger* (9. Aufl. 2022), § 327f Rn. 5.
[49] *Raue*, NJW 2017, 1841, 1844.

Produktbeobachtungspflichten die Schwachstelle entdeckt bzw. hätte entdecken können. Ein angemessener Zeitraum, um die Sicherheitslücke mit der gebotenen Sorgfalt zu beheben, ist dem Hersteller und darauf aufbauend dem ja meist von dem Hersteller verschiedenen Vertragspartner des Verbrauchers zuzubilligen, ehe der Verbraucher von der Nacherfüllung zu anderen Rechtsbehelfen wechseln kann. Dieser Gedanke klingt jedenfalls auch in § 327l Abs. 1 Satz 2 BGB an.

2. Der Inhalt der Unternehmerpflicht: Sicherstellen der Aktualisierung

Für den Vertragspartner des Verbrauchers sind diese Aktualisierungspflichten aus § 327f BGB, der nicht zugleich auch der Hersteller des Vertragsgegenstands ist, natürlich einigermaßen gefährlich. Er hat nämlich einerseits sicherzustellen, dass der Verbraucher das erforderliche Sicherheitsupdate rechtzeitig bereitgestellt bekommt. Andererseits kann er die anfänglich noch unbekannte Sicherheitslücke aber typischerweise selbst weder entdecken noch gar eine kompensierende Aktualisierung programmieren.[50] Er ist hierbei vielmehr auf Gedeih und Verderb dem Hersteller ausgeliefert und gerät dementsprechend seinem Vertragspartner gegenüber in die weitere Haftung, wenn der Unternehmer seine Produkte nicht angemessen beobachtet und die notwendigen Sicherheitsaktualisierungen nicht (rechtzeitig) liefert. Zwar mag diese Haftung häufig nicht auf Schadensersatz gerichtet sein, da der von dem Hersteller verschiedene Unternehmer selbst die unterbliebene Bereitstellung nicht zu vertreten hat (§ 280 Abs. 1 Satz 2 BGB) und er sich das Unterlassen des Herstellers regelmäßig auch nicht nach § 278 BGB zurechnen lassen muss.[51] Es bleibt aber die von einem unternehmerseitigen Vertretenmüssen unabhängige Möglichkeit, den Vertrag gem. § 327i Nr. 2 i.V.m. § 327m BGB zu beenden. Diese Vertragsbeendigung führt auf der Rechtsfolgenseite dazu, dass der Vertrag nach Maßgabe des § 327o BGB rückabzuwickeln ist. Für den Fall, dass der Verbrauchervertrag die Bereitstellung der Software nicht als Dauerschuldverhältnis, sondern als punktuellen Austauschvertrag konstruiert, hat der Unternehmer dem Verbraucher dabei nach § 327o Abs. 2 Satz 1 BGB dessen volle erbrachte Leistung zu erstatten, selbst wenn der Verbraucher das digitale

[50] BeckOGK BGB/*Fries* (Stand: 1.2.2023), § 327f Rn. 5.

[51] *Riehm/Abold*, CR 2021, 530 Rn. 42; *Rieländer*, GPR 2022, 28, 34 f.; s. aber *Hessel/Potel*, RDi 2022, 25 Rn. 15; BT-Drucks. 19/27653, S. 58 f.

Produkt womöglich jahrelang beanstandungslos nutzen konnte.[52]

Gegen dieses Problem mag der Rückgriff entlang der Lieferkette gemäß § 327u BGB zwar einen gewissen Schutz bieten. Nachdem – worauf in der Literatur bereits zutreffend hingewiesen wurde – dieser Rückgriff aber nur funktioniert, wenn entlang der gesamten Lieferkette deutsches Recht gilt und das nicht unbedingt häufig der Fall ist,[53] tut jedes Glied der Lieferkette ausgesprochen gut daran, sich vertragsgestalterisch, so gut es geht, gegen unkooperatives Verhalten des Herstellers abzusichern und auch nur solche Softwareprodukte und Waren mit digitalen Inhalten zu vertreiben, für die der Hersteller die ordnungsgemäße Beobachtung und Aktualisierung hinsichtlich der Sicherheit verbindlich zugesagt hat.

3. Für wie lange bleibt der Unternehmer zur Aktualisierung verpflichtet?

Gem. § 327f Abs. 1 Satz 3 Nr. 1 BGB besteht die Pflicht zur Sicherstellung von Aktualisierungen bei Verträgen, durch welche die Parteien die Bereitstellungspflicht als Dauerschuldverhältnis konstruieren („dauerhafte Bereitstellung eines digitalen Produkts“) während der gesamten Laufzeit des Dauerschuldverhältnisses, was wenig überrascht und letztlich der hergebrachten Regelung des § 535 Abs. 1 Satz 2 BGB entspricht.

Interessanter und freilich auch komplizierter ist demgegenüber die Regelung des § 327f Abs. 1 Satz 3 Nr. 2 BGB, der die Fälle betrifft, in denen der Unternehmer dem Verbraucher das digitale Produkt einmal bereitstellt und das entsprechende Vervielfältigungsstück sodann dauerhaft bei dem Verbraucher verbleibt. Hier dauert die Aktualisierungspflicht so lange an, wie es der Verbraucher aufgrund der Art und des Zwecks des digitalen Produkts und unter Berücksichtigung der Umstände und der Art des Vertrags erwarten kann. Dieser offene Tatbestand liegt natürlich einerseits in der Konsequenz des vertragstypenübergreifenden Regelungskonzepts

[52] *Riehm/Abold*, CR 2021, 530 Rn. 52; gelingt es demgegenüber dem Verkäufer einer Ware mit digitalen Elementen i.S.d. § 327a Abs. 3 BGB nicht, die Bereitstellung einer notwendigen Sicherheitsaktualisierung sicherzustellen, kann der Käufer den Kaufvertrag nicht nach § 327i Nr. 2 i.V.m. § 327m BGB beenden, sondern lediglich nach § 437 Nr. 2 i.V.m. §§ 346 ff. BGB von dem Vertrag zurücktreten. Die Rückabwicklung erfolgt in diesem Fall aufgrund von § 346 BGB, nach dessen Abs. 1 der zurückgetretene Käufer Ersatz für die zwischenzeitlich geleisteten Nutzungen zu leisten hat.

[53] *Heydn*, CR 2021, 709 Rn. 44.

der §§ 327 ff. BGB, geht andererseits aber auch auf Kosten der Rechtssicherheit,[54] was angesichts der Rückabwicklungsregelung in § 327o Abs. 2 BGB nicht unbedingt sachgerecht ist. Jedenfalls führt der unbestimmte Rechtsbegriff der für das konkrete Produkt berechtigten Verbrauchererwartungen stets zu einer Einzelfallbetrachtung.

Sicherlich kann der Aktualisierungszeitraum gem. § 327f Abs. 1 Satz 3 Nr. 2 BGB nicht mit der Verjährungsfrist für Nacherfüllungsansprüche gleichgesetzt werden.[55] Das folgt schon daraus, dass die erwartbare Gesamtlebensdauer eines Produkts und die Frist, innerhalb derer der Erwerber Ansprüche zur Beseitigung anfänglicher Mängel geltend machen kann, zweierlei sind. In der Literatur wird wesentlich darauf abgestellt, für welchen Zweck das digitale Produkt geschaffen wurde, namentlich zum langfristigen (z.B. Betriebssystem eines Computers) oder nur zum kurzfristigen Gebrauch (z.B. App für die Besucher eines Musikfestivals).[56] Bei längerfristig nutzbaren Programmen soll es auf eine – jeweils statistisch zu ermittelnde – übliche Supportdauer[57] oder aber auf die übliche Nutzungsdauer ankommen.[58] Ebenso wird man den Preis, den der Verbraucher für ein Computerprogramm entrichtet hat, in die Betrachtung miteinfließen lassen müssen.[59] Eine gewisse Orientierung mag auch die steuerliche Nutzungsdauer des Vertragsgegenstands bieten.[60] Es stellt sich allerdings die Frage, inwieweit dieser Ansatz auf die Situation der Verbrauchergeschäfte tatsächlich passt.

Für die Fälle, in denen das digitale Produkt mit einer Sache verbunden ist, wird ferner vorgeschlagen, „die aktualisierungspflichtige Zeit so zu bemessen, dass Verbraucher nicht durch fehlende Updates zur Ersetzung eines im Übrigen noch funktionstauglichen physischen Produkts veranlasst werden".[61] Das erscheint jedenfalls für die Firmware-Konstellationen sinnvoll, in denen die physische Sache ohne das mit ihr verbundene digitale Produkt nicht nutzbar ist. Zu weitgehend erscheint es allerdings, diesen Gedanken auf alle Fälle des § 327a Abs. 2 BGB auszudehnen. In diesem Fall hätte nämlich derjenige, der einen Computer mit

54 MüKoBGB/*Metzger* (9. Aufl. 2022), § 327f Rn. 10.
55 BT-Drucks. 19/27653, S. 59; MüKoBGB/*Metzger* (9. Aufl. 2022), § 327f Rn. 11.
56 MüKoBGB/*Metzger* (9. Aufl. 2022), § 327f Rn. 12.
57 MüKoBGB/*Metzger* (9. Aufl. 2022), § 327f Rn. 13.
58 *Heydn*, CR 2021, 709 Rn. 8.
59 BeckOGK BGB/*Fries* (Stand: 1.2.2023), § 327f Rn. 17; a.A. MüKoBGB/*Metzger* (9. Aufl. 2022), § 327f Rn. 13.
60 BeckOGK BGB/*Fries* (Stand: 1.2.2023), § 327f Rn. 16; *Heydn*, CR 2021, 709 Rn. 8.
61 BeckOGK BGB/*Fries* (Stand: 1.2.2023), § 327f Rn. 16.

bereits aufgespieltem Betriebssystem erwirbt, zugleich einen Anspruch auf Pflege dieses Betriebssystems, solange nur die Hardware noch einsatzfähig ist.

V. Bedeutung für die Ausgangsbeispiele

Insgesamt erfassen die §§ 327 ff. BGB und § 475b f. BGB die Sicherheitsprobleme einer für sich stehenden Software oder einer Firmware recht gut. Das Problem der unklaren Dauer der Aktualisierungspflicht nach § 327f Abs. 1 Satz 3 Nr. 2 BGB können die betroffenen Unternehmer und Hersteller abmildern, indem sie einen zeitlichen Sicherheitspuffer einplanen; immerhin können sie die entsprechenden Mehrkosten auf die Verbraucher abwälzen.[62] Problematisch bleibt allerdings der gesamte Bereich der Nicht-Verbraucherverträge – das beträfe von den Ausgangsbeispielen namentlich den Fall des Rhein-Pfalz-Kreises –, in denen die Erwerber digitaler Produkte gerade wegen der Aktualisierungen auf die individuelle Vertragsgestaltung, auf § 241 Abs. 2 BGB und ggf. auf die deliktische Produzentenhaftung angewiesen bleiben.

Ebenfalls problematisch bleiben einige Fälle von Hardware-Sicherheitslücken, und zwar selbst dann, wenn es sich um Verbrauchergeschäfte handelt. Betrachtet man nämlich die „Meltdown"- und „Spectre"-Konstellationen vor dem Hintergrund der §§ 327 ff. BGB, so dürfte es sich in deren Systematik wohl um einen Vertrag nach § 327a Abs. 2 BGB handeln. Hier ordnet § 327 Abs. 2 Satz 2 BGB allerdings an, dass das besondere Digitalvertragsrecht der §§ 327 ff. BGB lediglich für die Softwarekomponente gilt, nicht aber für die schadhafte Hardwarekomponente. Danach hätte – wenn man der Einfachheit halber die Anwendung von Kaufrecht unterstellt – der Käufer aus § 439 Abs. 1 BGB einen Nacherfüllungsanspruch, wenn die Hardware-Sicherheitslücke bereits bei Gefahrübergang bestand. Dabei kann der Unternehmer zum Zwecke der Nachbesserung sich tatsächlich eine Softwareaktualisierung liefern lassen, die den Hardwarefehler kompensiert. Tritt die Hardware-Sicherheitslücke demgegenüber erst später auf und kann sie auch nicht als im Zeitpunkt des Gefahrübergangs bereits im Kern angelegt angesehen werden, besteht keine Pflicht nach § 327f Abs. 1 BGB, dem Käufer eine Softwareaktualisierung zur Verfügung zu stellen, die den Hardwarefehler ausgleicht.

[62] BeckOGK BGB/*Fries* (Stand: 1.2.2023), § 327f Rn. 4.

VI. Zusammenfassung der wesentlichen Ergebnisse

Bei einem Vertrag nach § 327 Abs. 1 BGB hat der Verbraucher einen primären Leistungsanspruch, dass eine ihm bereitgestellte Software im Hinblick auf die Sicherheit gegen Angriffe von außen dem Standard genügt, der für eine Software dieser Art üblich ist und von dem Verbraucher legitimerweise erwartet werden kann. Das gilt auch, wenn die Software nicht allein, sondern nach Maßgabe von § 327a Abs. 1 und 2 BGB gemeinsam mit anderen Leistungen als digitalen Produkten vertrieben wird. Ein entsprechender Primäranspruch besteht nach § 475b Abs. 4 Nr. 1 BGB auch bei Verbrauchsgüterkaufverträgen über Waren mit digitalen Inhalten sowie bei Kauf-, Werk-, Miet- und Herstellerleasingverträgen über Software und Waren mit digitalen Elementen zwischen Unternehmern.

In allen diesen Konstellationen besteht ein Anspruch auf Bereitstellung einer Sicherheitsaktualisierung, wenn die Software oder die Ware mit digitalen Inhalten bereits zur Zeit von Bereitstellung, Überlassung oder Gefahrübergang hinter diesem geschuldeten Sicherheitsstandard und damit der vertraglich geschuldeten Soll-Beschaffenheit zurückbleibt.

Bei Verbraucherverträgen über die Bereitstellung von Software und ebenso bei Verbrauchsgüterkaufverträgen über Waren mit digitalen Elementen hat der Verbraucher darüber hinaus einen Anspruch auf Nacherfüllung, wenn der Vertragsgegenstand später hinter diese Soll-Beschaffenheit zurückfällt und der Vertragspartner nicht sicherstellt, dass dem Verbraucher eine für die Erhaltung der Soll-Beschaffenheit erforderliche Sicherheitsaktualisierung bereitgestellt wird.

Einen Anspruch auf Beseitigung nachträglicher Sicherheitsmängel gibt es im unternehmerischen Verkehr nach § 535 Abs. 1 Satz 2 BGB bei Miet- und Herstellerleasingverträgen über Software und Waren mit digitalen Elementen. Im Übrigen kann ein Unternehmer eine nachträgliche Sicherheitsaktualisierung an sich nur verlangen, wenn und soweit dies vertraglich vereinbart ist, es sei denn, man möchte entsprechende Leistungsansprüche aus § 241 Abs. 2 BGB oder aus der deliktischen Produzentenhaftung ableiten.

Hinter der geschuldeten Soll-Beschaffenheit bleibt eine Software oder eine Ware mit digitalen Elementen bereits anfänglich zurück, wenn sie im Zeitpunkt von Bereitstellung, Überlassung oder Gefahrübergang eine zu dieser Zeit schon bekannte

Sicherheitslücke aufweist, darüber hinaus aber auch hinsichtlich noch unbekannter Sicherheitslücken, die der Hersteller bei einer Programmierung nach dem Stand der Technik für dieses Produkt hätte erkennen und vermeiden können.

Eine Sicherheitsaktualisierung wird im Sinne von § 327f Abs. 1 BGB erforderlich und ist von dem Vertragspartner des Verbrauchers sicherzustellen, sobald der Hersteller bei Beachtung der produzentenhaftungsrechtlichen Produktbeobachtungspflichten eine Sicherheitslücke erkennen kann, spätestens aber, sobald eine bislang unentdeckte Sicherheitslücke öffentlich bekannt wird. Wie lange diese Aktualisierungspflicht des Unternehmers aufgrund von § 327f Abs. 1 Satz 3 Nr. 2 BGB andauert, hängt sehr stark von den Umständen des einzelnen Falls ab.